INFORMATION ASSURANCE

CERTIFICATION AND ACCREDITATION

(C&A)

PUBLICATION

VOLUME I

Introduction to Certification and Accreditation

DEPARTMENT OF THE NAVY (DoN)
INFORMATION ASSURANCE (IA)
PUBLICATION

MODULE 5239-13 VOL I

Distribution:

Electronic versions of this document may be downloaded via anonymous ftp from infosec.navy.mil or via the DoN INFOSEC/IA Web Site on the NIPRNET at https://infosec.navy.mil and on the SIPRNET at https://infosec.navy.smil.mil

For further assistance, the INFOSEC Technical Assistance Center (ITAC) may be reached at:

Commercial 1-800-304-4636
DSN 588-5428 / 4286

FOREWORD

Naval Information Assurance Program Publications (IA Pub) are issued by the Chief of Naval Operations (CNO) N643. The IA Pub series provides modules that guide the implementation of the policy direction established in Chief of Naval Operations Instruction (OPNAVINST) 5239.1B. These modules provide procedural, technical, administrative, and supplemental guidance for all information systems, whether business or tactical, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or receipt of data. Each module focuses on a distinct subject and describes a standard methodology for planning, implementing, and executing that element of the IA program within the Department of the Navy (DoN).

This module, "Information Assurance Certification and Accreditation (C&A) Publication, Volume 1, " provides the DoN IA C&A approach.

Reviewed and Approved by:

CNO N643 Louise Davidson 9 JAN 2001

TABLE OF CONTENTS

TABLE OF FIGURES

SECTION 1.0
INTRODUCTION

This module introduces the Department of the Navy (DoN) Information Assurance (IA) Certification and Accreditation (C&A) Publication (IA Pub). This Pub extends the Chief of Naval Operations (CNO) policy directed in OPNAVINST 5239.1B by providing IA guidance, procedures, and processes to assist the DoN in implementing its Information Assurance C&A program.

1.1 SCOPE AND PURPOSE

The IA Pub 5239-13 series is composed of 3 volumes. Each volume provides guidance and information applicable to a specific area of the DON C&A process. Due to the length and detail of the information required to understand the DoN's approach to C&A, this publication has been divided into three volumes.

This volume introduces and summarizes the C&A process. It applies to systems/components processing unclassified, sensitive but unclassified, and classified information. The IA Pub 5239-13 series addresses the following information:

Volume I: Introduction to Certification and Accreditation

Volume II: Certification and Accreditation of Site, Installed Program of Record, and Locally Acquired Systems

Volume III: Certification and Accreditation of Program of Record Systems

By using the information in these volumes, the personnel involved in the acquisition and operation of DoN systems will have a common understanding of C&A principles, concepts, and processes.

The DoN C&A program is targeted for the following audiences:

- **Designated Approving Authority (DAA)**: Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority. (See discussion below regarding Developmental DAA and Operational DAA.)

- **Program Manager (PM)**: The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the Information Technology (IT) system.

- **Certification Authority (CA) (Certifier)**: Official with the responsibility of stating the extent to which a system/component meets a set of specified security requirements.

- **Certification Agent**: Individuals or organization performing a technical evaluation of the system/component's compliance with stated security requirements, identifying and assessing the risks associated with operating the system/component, and coordinating the certification activities to include the final System Security Authorization Agreement (SSAA). This role may be assigned to various entities based upon complexity of the certification level of effort.

- **Information System Security Manager (ISSM)**: The Operational DAA's principal advisor on IA matters.

- **Information System Security Officer (ISSO)**: The person responsible to the DAA for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with System Security Officer.

- **System Support activity/Software Support Activity (SSA**): the organization, acting on behalf of the Program Manager, providing life-cycle support for an operational system.

- **User Representative**: The individual or organization that represents the user or user community in determining information system security requirements.

The DoN establishes two types of DAAs, Developmental and Operational. The Developmental DAA (DDAA) supports the program acquisition during the design and development of a system/component and accredits systems prior to their deployment. The Operational DAA (hereafter simply referred to as the DAA) is the ultimate approving authority for system operation at a specific site. The ISSM, PM, CA, ISSO, and Certification Agent interact with the DAA in providing enough evidence to make a risk acceptance decision.

The PM is the system/component developer responsible for ensuring the security design. The DAA, ISSM, CA, ISSO, and Certification Agent interact with the PM to support requirements definition and security engineering.

The Certification Authority reviews the C&A package prepared by the Certification Agent and issues the certification statement. This statement describes the extent to which the system/component meets the stated specified set of security requirements and is provided to support the accreditation process. The CA should have some level of confidence in the Certification Agent who provides the verification information (i.e., Phase 2 SSAA) for certification.

The Certification Agent supports the CA in verifying the security requirements. The Certification Agent supports the PM by providing security engineering during the development of the system/component and assists in development of the SSAA for submission to the DAA.

The roles and responsibilities for the ISSM and ISSO are detailed in separate DoN IA Publications. The ISSO is an operational designation and is not involved in Program of Record acquisition. The ISSO is involved in the site and locally acquired acquisition as defined in the definition and described in the appropriate IA Publications. Figure 1-1, C&A Roles, shows transitional relationships. In this figure, SSA refers to the system or Software Support Activity acting on behalf of the PM.

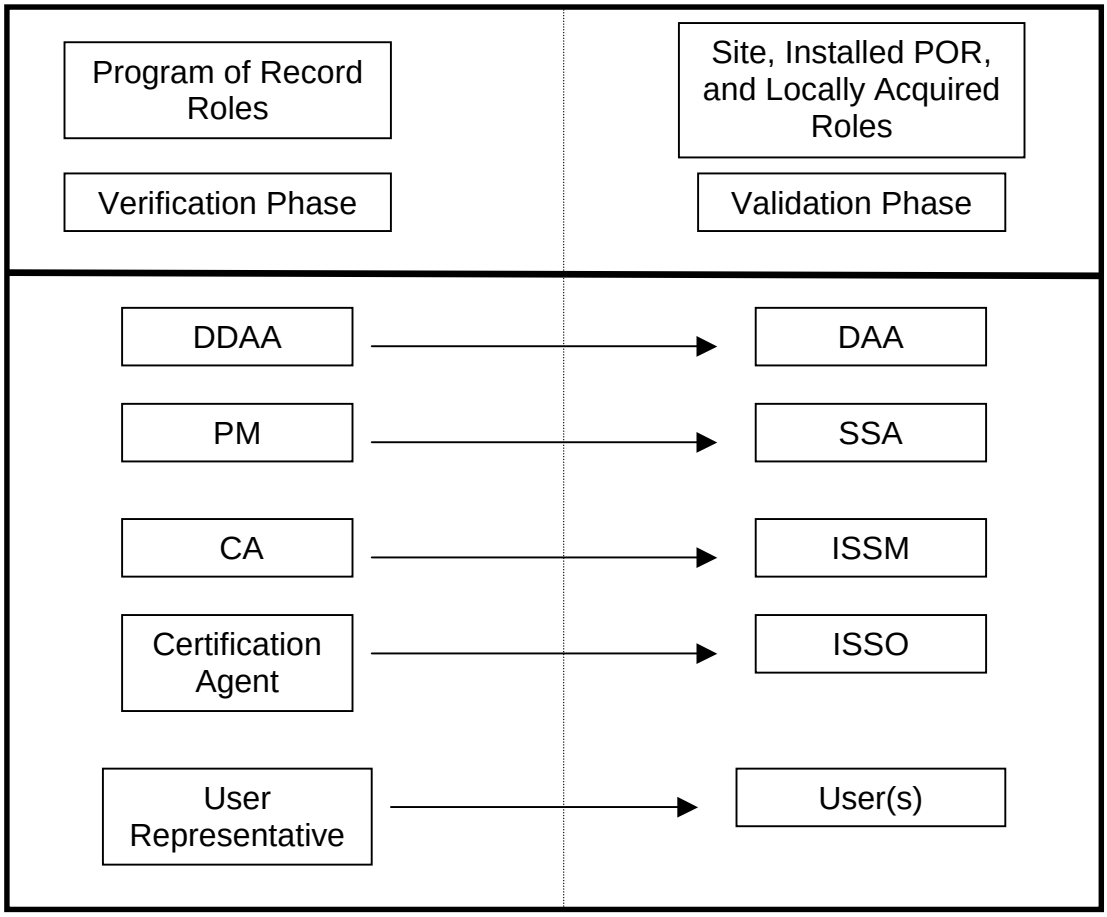

Figure 1-1, C&A Roles

1.2 CERTIFICATION AND ACCREDITATION DEFINITION

Certification and Accreditation are key terms used in this publication. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009, National Information Systems Security (INFOSEC) Glossary, defines these terms as follows:

> Certification is the “comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements.”

Accreditation is the “Formal declaration by a Designated Approving Authority (DAA) that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.”

1.3 DEPARTMENT OF DEFENSE INFORMATION TECHNOLOGY SECURITY CERTIFICATION AND ACCREDITATION PROCESS (DITSCAP)

The DITSCAP applies to the acquisition, operation and sustention of any DoD system that collects, stores, transmits, or processes unclassified or classified information. It applies to any IT or system life cycle, including the development of new IT systems, the incorporation of IT systems into an infrastructure, the incorporation of IT systems outside the infrastructure, the development of prototype IT systems, the reconfiguration or upgrade of existing systems, and legacy systems. It may be adapted to include existing system certifications, evaluated products, new security technology or programs, and adjust to the applicable standards.

The DITSCAP provides high level definition of a process that standardizes all activities leading to a successful accreditation. The principle purpose of that process is to protect and secure the entities comprising the Defense Information Infrastructure (DII). Standardizing the process minimizes risks associated with nonstandard security implementations across shared infrastructure and end systems. The DITSCAP consists of four phases: Definition, Verification, Validation, and Post-Accreditation.

The DITSCAP methodology applies to all DoD information systems requiring C&A throughout their life cycle. It is designed to be adaptable to any type of IT system and any computing environment and mission. The DITSCAP may be mapped to any system life-cycle process but is independent of the life cycle strategy. The DITSCAP is designed to adjust to the development, modification, and operational life cycle phases. Each new C&A effort begins with phase 1, Definition, and ends with phase 4, Post Accreditation, during which follow-up actions ensure that the approved system or system component continues to operate in its computing environment in accordance with its accreditation. The DITSCAP states that “activities defined in these four phases are mandatory. However, implementation details of these activities *may be tailored*, and where applicable, integrated with other acquisition activities and documentation.”

1.4 INFORMATION ASSURANCE ACQUISITION POLICY

Effective 1 January 2001, preference shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting national security information) which have been evaluated and validated, as appropriate, in accordance with:

- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangement;

- The National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program; or

- The NIST Federal Information Processing Standard (FIPS) validation program.

By 1 July 2002, the acquisition of all COTS IA and IA-enabled IT products to be used on the systems specified in the paragraph above, shall be limited only to those which have been evaluated and validated in accordance with the criteria, schemes, or programs specified in the three sub-bullets.

SECTION 2.0
UNDERSTANDING CERTIFICATION

It is DoN Information Assurance (IA) Policy that information and resources shall be appropriately safeguarded at all times, to support defense in depth across DoN and DoD. Safeguards shall be applied such that information and resources maintain the appropriate level of confidentiality, integrity, availability, and accountability based upon mission criticality, level of concern, and classification or sensitivity level of information entered, processed, stored, and/or transmitted. The safeguarding of information and information systems shall be accomplished through the employment of defensive layers that include the IA disciplines as discussed in OPNAVINST 5239.1B and defined in IA Publication 5239-01.

Certification is the means by which these safeguards are assessed. Certification is applied to provide an approving authority with the details required for making an informed decision about the protection and defense of the information and/or system.

2.1 DEFINITION-BASED PERSPECTIVE

In order to establish an approach that ensures that safeguards are applied to a system or component certification, the meaning of "certification" must be understood. NSTISSI 4009 defines certification as:

> "The comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements."

Common themes in the definition of certification that are consistent with any approach are:

- It is a comprehensive evaluation
- It is made in support of the accreditation process
- It establishes the extent to which a set of specified security requirements is met

This definition encompasses two distinct approaches to certification based upon the design and implementation of a system/component that supports a cost effective method for implementing the DoN IA Policy, i.e., OPNAVINST 5239.1B. These two approaches are (1) system or component certification, and (2) operational environment certification. These will be discussed in sections 2.2 and 2.3, respectively.

2.1.1 A Comprehensive Evaluation

A comprehensive evaluation is complete and ignores no element of the system, while also providing sufficient detail to adequately understand the behavior of the system.

A comprehensive evaluation examines both the security functions (i.e., the security behavior) of a system and the assurances that those functions are correctly implemented and satisfy the security objectives as discussed in ISO 15408, Common Criteria. There are varying levels of effort that can be applied in an evaluation process. The goal is to conduct an evaluation at the level of effort that yields sufficient information for the DAA to make an informed decision.

Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510 “Department of Defense Global Information Grid Information Assurance” provides three distinct definitions for Information Assurance Levels of Concern:

High: Systems that require the most stringent protection measures and rigorous countermeasures. The DoN considers these systems/components as equating to Common Criteria Evaluated Assurance Level (EAL) 5 and above. These system/components are National Security Agency products and security systems/components provided to the fleet by the DoN Certification Authority. This does not exclude the ability of a Program of Record to develop an EAL 5 or above component and have it certified by the DoN Certification Authority. These systems fall into the mission critical category and may cross classification domains and are therefore applicable to the SECRET/TOP SECRET and Below Interoperability (SABI/TSABI) and/or coalition interests.

Medium: Systems that require layering of additional safeguards above the DoD minimum standard (i.e., Basic). The DoN considers these systems/components as equating to at least the Common Criteria EAL 3. These systems/components are SYSCOM Program of Record acquisitions that fall into Mission Critical Category I, II, or III.

Basic: Systems that require implementation of the DoD minimum standard. The DoN considers these systems/components as equating to Common Criteria EAL 1 or 2. These are Locally Acquired systems/components that provide administrative or mission support services. (See IA Pub 5239.13 Vol II).

2.1.2 Made in Support of the Accreditation Process

Certification and its associated activities are performed for the purpose of providing a DAA with the information required for making an informed accreditation decision. The Certification Authority issues a statement regarding the extent to which a system/component meets a set of specified requirements. Certification evidence supports the accreditation process. This evidence addresses the system/component's ability to protect and defend the information processed, stored, and/or transmitted on that system/component.

Certification tasks should begin during system/component development at the point in the life cycle when system and component details are available and CT&E can be executed. A detailed analysis of certification activities in support of the accreditation process is provided in sections 2.2 and 2.3 below. Certification is most efficient when the certification information can be used in multiple accreditations, i.e., either in a type accreditation or site accreditation process. Section 3 discusses the concept of accreditation.

Type accreditations are built upon the concept that systems (or integrated group of components) are duplicated in design, implementation, and configuration. Thus, the behavior of their security functions can be certified as being identical. Additionally, if these systems (or integrated group of components) are implemented in a similar operational environment, similar assumptions about the operational risk can be made. More detail on the application of certification in support of accreditation can be found in the following sections of this publication.

2.1.3 Extent to which a Set of Specified Security Requirements is met

Security requirements are intimately tied to the functionality requirements of a system. The critical function of a Certification Agent or ISSM/ISSO is to examine through demonstration, inspection, and/or analysis the extent to which an information system meets a set of specified security requirements (as specified by the DAA and governing instructions and directives). The focus of these requirements is on the need to deploy effective countermeasures that meet the IA objectives of sufficient confidentiality, integrity, availability, and accountability. The Certification Authority approves the evaluation efforts

completed by a Certification Agent and provides a formal statement that establishes the extent to which a set of specified security requirements is met.

This C&A process, conducted in support of the DoN IA Program, has an established IA checklist. The checklist is derived from the experience of DoN Certification Agents and Fleet representatives and is based upon known threat activity. The checklist contains the minimal security requirements and is most appropriate for systems requiring a Basic level of assurance. The checklist can be found in IA Publication 5239-13 Volume II.

- Basic assurance systems require a checklist and use of a network vulnerability tool (e.g., Internet Security Scanner, CyberCop).
- Medium assurance systems require at least a Common Criteria EAL-3 or above and use of a network vulnerability tool.
- High assurance systems require the equivalent of at least a Common Criteria EAL-5 and above (see IA Publication 5239-13 Volume III) with an automated vulnerability tool once the system is installed on a network.

The DoN IA Program will maintain a list of IA requirements (Naval IA Publication 5239-18, *Information System Security Requirements under development*) that are drawn from National, DoD, and Service/Agency instructions. Security practitioners can use 5239-18 for a consolidated list of IA objectives and requirements that are drawn from National, DoD, and Service/Agency instructions for application to a system/component.

2.2 SYSTEM OR COMPONENT CERTIFICATION

Either systems or their individual components can be certified. Commercial products, that are components of a system, are, by national policy, evaluated using ISO Standard 15408, *The Common Criteria for Information Technology Security Evaluation*. Program Managers may integrate evaluated systems/components into their acquisition. Program Managers developing systems/components should have their systems/components certified.

While reviewing the NSTISSI 4009 definition of *certification* from the perspective of establishing a distinctive, cost effective solution to implementing the DoN IA Policy key phrases become evident:

> "The comprehensive evaluation of the **technical** and non-technical **security features** of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which **a particular design** and implementation meets a set of specified security requirements."

The technical security features are those services and functions identified under the Communications Security (COMSEC), Computer Security (COMPUSEC), and Emissions Security (EMSEC) INFOSEC disciplines. These technical security features are part of the system's particular design.

Restructuring this definition, from this perspective, provides the following:

> "The comprehensive evaluation of the technical security features of an information system...to establish the extent to which a particular design meets a set of specified security requirements."

Focusing on this portion of the Certification definition, the Program Manager can direct resources to assess systems or components, i.e., a particular design of a specific system against a set of specified requirements. For example, if a Certification Agent were to assess a particular firewall product against a set of specified security requirements, a "System or Component Certification Statement" could be issued by the Certification Authority. This Certification Statement would be valid for that particular firewall in any infrastructure of a DoN organization as long as the same system and security configurations were used.

A certification is usually accompanied with identified assumptions about the operational environment. The system or component may be certified to meet a set of specified technical requirements, but was designed to that particular set of technical requirements with the assumption that a minimal set of non-technical requirements would be implemented at the operational site. For instance, a system may be designed to operate in the system high mode with the assumption that the operating environment will enforce physical security that only allows users cleared to the system high classification level physical access to the system.

2.3 OPERATIONAL ENVIRONMENT CERTIFICATION

While reviewing the NSTISSI 4009 definition of *certification* from the perspective of establishing a distinctive, cost effective solution to implementing the DoN IA Policy a final key phrase becomes evident:

> "The comprehensive evaluation of the technical and **non-technical security features** of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and **implementation** meets a set of specified security requirements."

The non-technical security features are those activities identified under the Physical Security (PHYSEC), Personnel Security (PERSEC), Procedural Security (PROSEC), and Security Education Training and Awareness (SETA) INFOSEC disciplines. These non-technical security features are part of the system's implementation that supports the protection and control of the information and resources from unauthorized disclosure, modification, or denial of service. Non-technical security features may be implemented to reduce the level of risk resulting from non-existent or weak technical security features.

Restructuring this definition from this perspective provides the following:

> "The comprehensive evaluation of the non-technical security features of an information system...to establish the extent to which an implementation meets a set of specified security requirements."

Focusing on this portion of the Certification definition, the Program Manager or ISSM can allocate resources to fielding systems in a secure environment, i.e., and an implementation of a specific system compliant with a set of specified requirements. For example, if the ISSM, ISSO, certification agent and other individuals in support of the DAA were to install a certified firewall product in an operational environment, they could assess only the firewall configuration and non-technical set of specified security requirements. The ISSM may issue an "Operational Environment Certification" by completing the SSAA during Phase 3 of the C&A process. Additionally, as will be shown in the next section, Operational Environment Certification can be useful when developing a Type Accreditation Statement and may further extend resources.

2.4 APPLICATION OF THE TWO CERTIFICATION APPROACHES

The DoN may field a single instance of an information system where a single C&A was performed, or several fieldings of an information system where the DAA has decided to perform a complete C&A effort on each implementation (see Figure 2-3). The DoN can benefit by tailoring the IA C&A process for a particular system that will be installed in multiple instances to include the system or component certification approach. By segregating the technical set of specified security requirements to a particular design, a comprehensive evaluation of the technical security requirements may be performed only once. Any Certification Authority or DAA may reuse the results of this evaluation in each and every instance of the system's implementation (see Figure 2-4). The reason this may occur is that the designed technical security features are not going to change, i.e., they are designed into the system.

The DoN can benefit by tailoring the IA C&A process for a particular system that will be installed in multiple instances to include the Operational Environment Certification approach. By segregating the non-technical set of specified security requirements to a particular implementation, a comprehensive evaluation of the non-technical set of security requirements may be performed a limited number of times (depending on the assurance required by the DAA). Assessment of the non-technical security requirements in specified types of implementations (to include the environment) can be used to issue a "Type Accreditation" (see section 3.2). The Type Accreditation basically indicates that if the system (i.e., technical set of specified requirements) is installed and configured in a particular environment (i.e., non-technical set of specified requirements), the system is approved to operate. As can be seen, this statement can be issued for a single information system that is installed in multiple instances (i.e., tens, hundreds).

This does not imply that each and every DoN system C&A effort must perform a system or component certification. The correct IA C&A approach should be agreed upon by the DAA, Certification Authority, PM, and the User Representative during Phase 1.

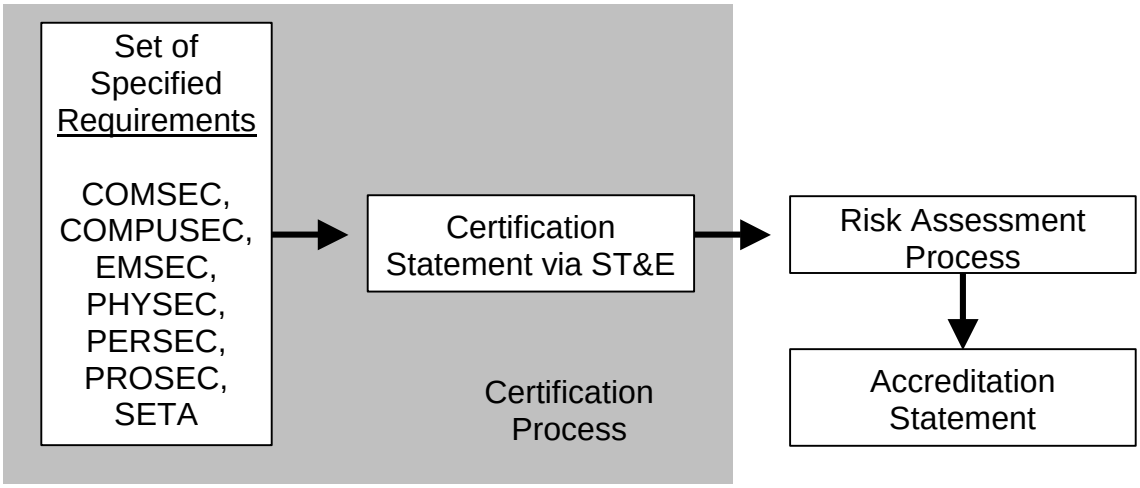

Figure 2-1 Single Implementation Approach

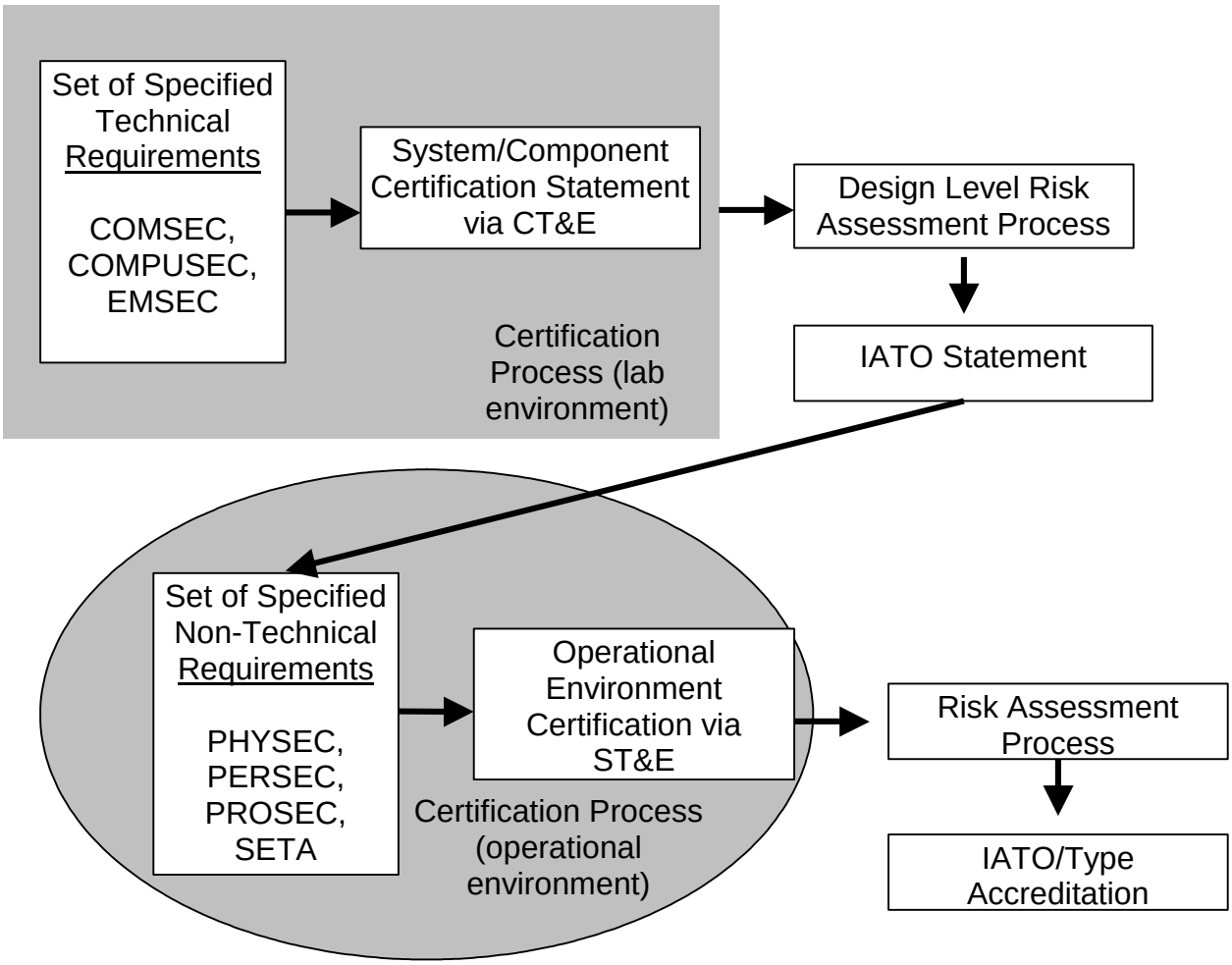

Figure 2-2 Multiple Implementation Approach

SECTION 3.0
UNDERSTANDING ACCREDITATION

It is DoN Information Assurance Policy that information and resources shall be appropriately safeguarded at all times, to support defense in depth across DoN and DoD. Safeguards shall be applied such that information and resources maintain the appropriate level of confidentiality, integrity, availability, and accountability based upon mission criticality, level of required IA, and classification or sensitivity level of information entered, processed, stored, and/or transmitted. The safeguarding of information and systems shall be accomplished through the employment of defensive layers that include the IA disciplines (see DoN IA Publication 5239-01).

Accreditation is the authorization, granted by the DAA, that permits a system to process, store, and/or transmit information. This authorization is granted based upon information gathered during the certification process and concerns the protection and defense of the information and/or system.

3.1 DEFINITION-BASED PERSPECTIVE

In order to establish a common understanding of the meaning of "accreditation" we will analyze the NSTISSI 4009 definition of accreditation:

> "Formal declaration by a Designated Approving Authority (DAA) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk."

The definition of accreditation addresses specific topics.

- A formal declaration by a DAA
- Approval to operate
- A particular security mode
- Using a prescribed set of safeguards
- An acceptable level of risk

This definition includes a complete list of activities that must occur to achieve accreditation of a system.

3.1.1 A Formal Declaration by a DAA

This portion of the definition of accreditation implies a recognized statement from the DAA. The DAA must sign a statement approving the system to operate. This statement should address all of the aforementioned specific concerns identified in the definition. Additionally, all four parties to the SSAA should sign the SSAA prior to accreditation approval.

3.1.2 Approval to Operate

The accreditation statement states the DAA's acceptance of risk in the protection and defense of the information and system(s). There are two types of approvals to operate, i.e., Approval to Operate or an Interim Approval To Operate (IATO).

Approval to operate indicates that conditions required to accredit the system set by the D/DAA have been satisfactorily designed and implemented. Approval to operate may be issued for a single instance of a system (System Accreditation) or multiple instances (Type Accreditation) if the system is installed in an approved configuration and a specified type of operating environment. Approval to operate may also be issued for a collection of systems at a single site. This is known as a Site Accreditation. The systems that are included in the Site Accreditation must be clearly identified.

Interim Approval to Operate (IATO) can be requested when: testing needs to be completed at an operational site, an operating a system has not completed its certification and accreditation, or the D/DAA has reservations regarding the operation of the system at the currently identified residual risk. A certification agent or ISSM usually requests an IATO from the D/DAA to validate the extent to which a system meets a set of specified security requirements in an operational environment. When testing is completed in the operational environment the DAA will make the decision to allow or deny the system to continue to operate.

An IATO may be granted or extended when accreditation is not immediately declared. In such instances, the D/DAA will either identify additional countermeasures to be designed and/or implemented, or require that failed countermeasures (as identified by the certification process) be corrected before an accreditation is issued. An IATO usually specifies how long the system may operate while achieving compliance with the D/DAA's requirements. An IATO may not exceed one-year.

3.1.3 A Particular Security Mode

The particular security mode in which the system is approved to operate will be one of the following NSTISSI 4009 defined modes. Additionally, specific differences between the modes have been italicized and bolded.

- **Dedicated**: Information system security mode of operation wherein each user, with direct or indirect access to the system, its peripherals, remote terminals, or remote hosts, has all of the following:
  - valid security clearance for all information within the system;
  - formal access approval and signed non-disclosure agreements for all the information stored and/or processed (including all compartments, sub-compartments, and/or special access programs); and
  - valid need-to-know for all information contained within the information system.

When in the dedicated security mode, a system is specifically and exclusively dedicated to and controlled for the processing of one particular type or classification of information, either for full-time operation or for a specified period of time.

- **System High**: Information system security mode of operation wherein each user, with direct or indirect access to the information system, its peripherals, remote terminals, or remote hosts, has all of the following:
  - valid security clearance for all information within an information system;
  - formal access approval and signed nondisclosure agreements for all the information stored and/or processed (including all compartments, sub-compartments and/or special access programs); and
  - valid need-to-know for ***some*** of the information contained within the information system.

- **Compartmented**: Information system security mode of operation wherein each user with direct or indirect access to a system, its peripherals, remote terminals, or remote hosts has all of the following:

  - valid security clearance for the ***most restricted*** information processed in the system;
  - formal access approval and signed non-disclosure agreements for **that** information ***to which a user is to have access***; and
  - valid need-to-know for information ***to which a user is to have access***.

- **Multi-Level Security (MLS)**: Information system security mode of operation wherein all the following statements are satisfied concerning the users who have direct or indirect access to the system, its peripherals, remote terminals, or remote hosts:
  - ***some users do not have*** a valid security clearance for all the information processed in the information system;
  - all users have the ***proper*** security clearance and appropriate formal access approval for that information to which they have access; and
  - all users have a valid need-to-know ***only for information*** to which they have access.

3.1.4 Using Prescribed Set of Safeguards

The system receives an approval to operate based upon the use of the designed and implemented set of safeguards. The set of safeguards are those that are validated during the certification process (see paragraph 2.1.3). These requirements are coordinated and agreed upon with the DAA early during the Definition phase (DITSCAP Phase 1) of system development.

3.1.5 At an Acceptable Level of Risk

The key to accreditation of a system is establishing an acceptable level of risk. During the certification process activities, the extent to which a system meets a set of specified requirements is assessed. Additionally, a risk assessment is conducted and a statement of Residual Risk is prepared. Residual risk is "the portion of risk remaining after security measures have been applied to determine potential impact to mission operations." The residual risk assessment informs the DAA of the level of risk that is being accepted in the operation of the system for which the DAA is responsible.

IA Publication 5239-16, Risk Assessment, discusses the activity of risk assessment within the C&A process. The discussion of risk focuses on the potential impacts of disclosure, modification, and/or denial of service as exploited by a weakness in the design and/or implementation of the set of specified security requirements.

The DAA will determine if the risk identified through the development of the SSAA is acceptable. If the risk is acceptable, the DAA will issue an accreditation statement approving the system to operate in a particular security mode using the approved set of requirements. If the risk is not acceptable, the DAA may issue an IATO in a particular security mode (which could be lower than the target) with additional restrictions while required countermeasures are being

designed and implemented. Also, if the risk is not acceptable and the DAA does not want to issue an IATO due to the level of risk, the DAA may deny approval to operate until the risk management process reduces the risk to acceptable levels.

3.2 APPLICATION OF THE ACCREDITATION STATEMENT

There are three forms of the accreditation statement, i.e., the System Accreditation Statement, Type Accreditation Statement, and Site Accreditation Statement. Depending on the scope of the implementation of the system(s) any of these forms may be applicable. Again, this should be agreed upon by the DAA early in the definition phase of the IA C&A process.

System Accreditation is a statement issued for the approved operation of a single instance of a system.

Type Accreditation is a statement issued for the approved operation of multiple instances of a system. This statement usually specifies the nature of the Type Accreditation, i.e.; the system must be installed and configured in accordance with a documented set of requirements. Figure 3.1, Accreditation Approach, provides a block diagram of the activities and decisions that flow from the accreditation process.

Site Accreditation is a statement issued for the approved operation of all systems within a defined accreditation boundary. A single Site SSAA collects the SSAAs for the security domains of the site. A security domain is comprised of the set of systems operating under similar security policies. Since different classification levels have different security policies, they are distinct domains. For a typical Site SSAA, there would be domain SSAAs for the Sensitive but Unclassified, Confidential, and Secret domains for the systems at that site. Unique domains, such as those containing multilevel guards reviewed under SABI would have their individual SSAAs.

Site, Program of Record, Installed Program of Record/Locally Acquired SSAA templates are available. The concepts behind the content and structure of these templates are discussed in the appropriate volumes to this publication. These templates are provided for general guidance.

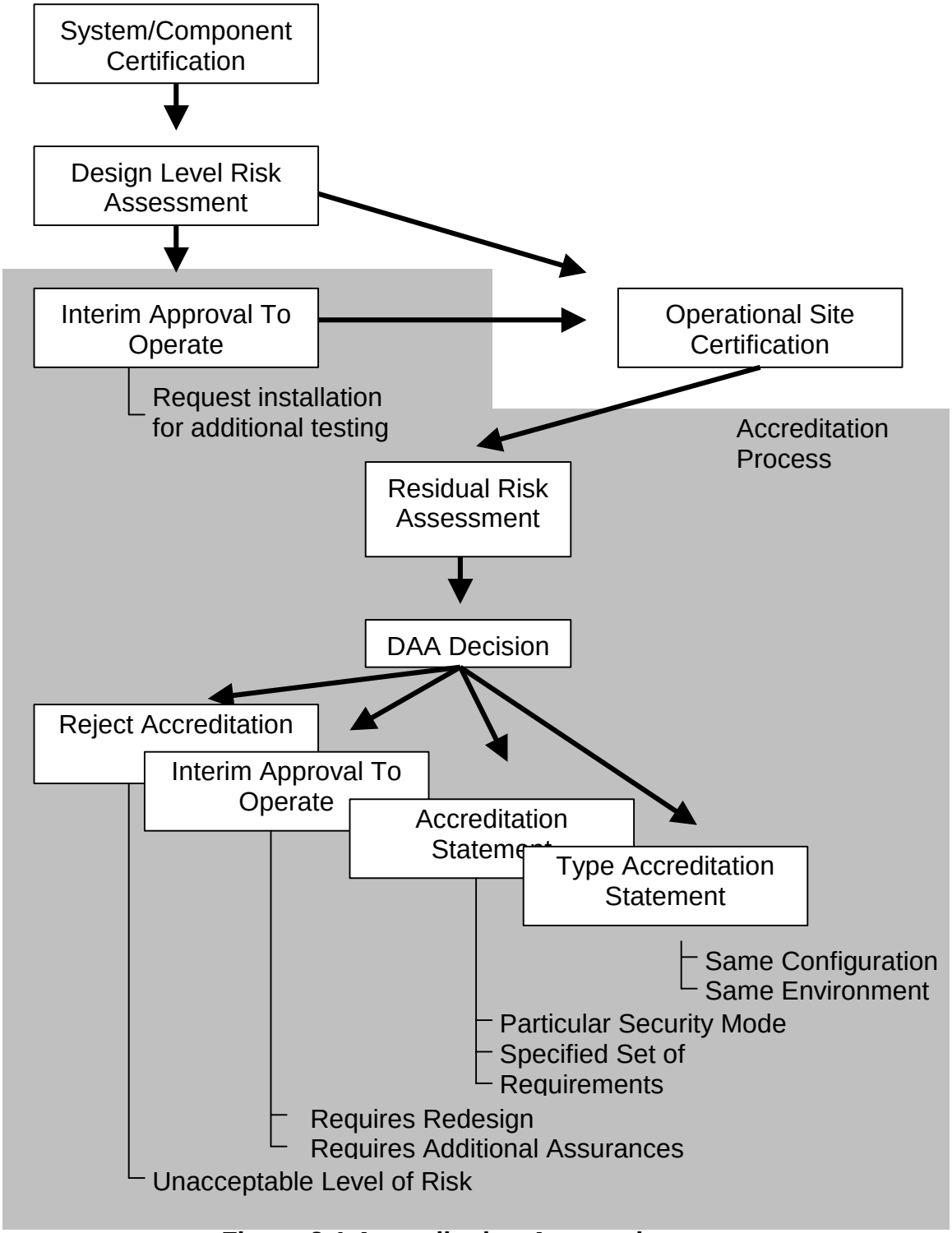

Figure 3-1 Accreditation Approach

SECTION 4.0

VOLUME II AND III

This section provides guidance on selecting the appropriate volume of IA Pub 5239-13 to satisfy the requirement to certify and accredit DoN systems. Volume II of 5239-13 provides an IA C&A checklist that satisfies the certification level of effort for systems that may only require a Basic level of IA. Volume III of 5239-13 provides a C&A process for systems that require increasing levels of information assurance. Both volumes are within the scope of the DoN IA Program, implement the DITSCAP and provide the assurances necessary to approve the operation of systems. It is within the purview of the DAA to require, within the bounds of higher echelon policies, additional or fewer security safeguards. Ultimately, the DAA must make a decision on whether to accept residual risk. Since risk tolerance can vary from DAA to DAA, the impact to community risk from interconnected systems that are outside the DAA's purview must be considered. Figure 4-1 provides a general guide to the selection of the appropriate level of C&A effort. The DAA, with support from the CA, should decide on the level of detail that is appropriate for determining the risk in operating a system.

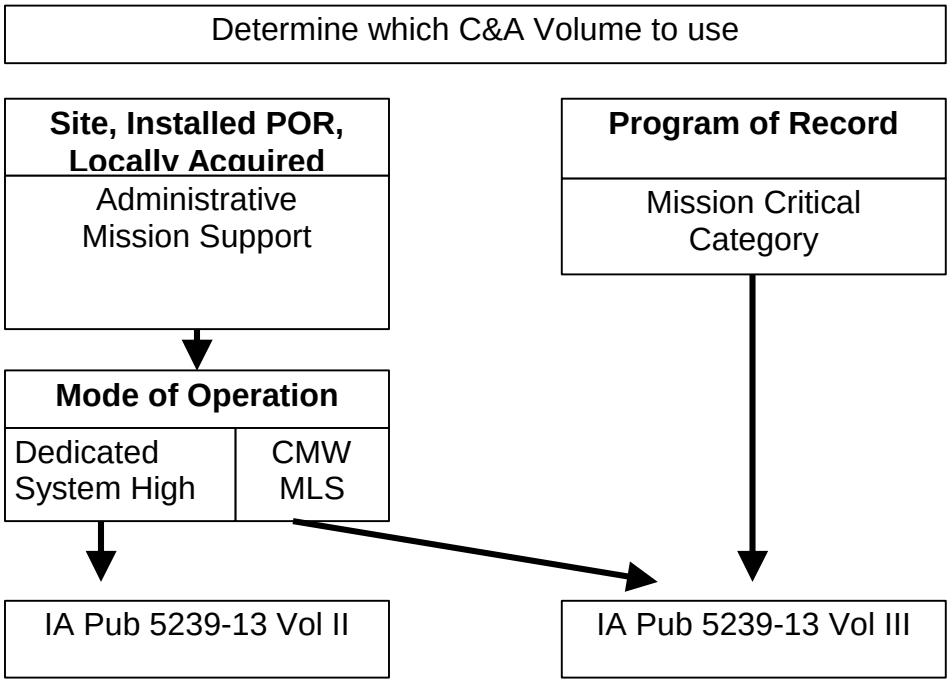

Figure 4-1 Selecting the Appropriate IA Pub 5239-13 Volume

IA Pub 5239-01 defines five categories of information systems, i.e., Administrative and Mission Support, Mission Critical Category I, II, and III. As a general rule Administrative and Mission Support information systems are locally acquired.

- Locally acquired systems that operate in the dedicated or system high mode should use IA Publication 5239-13 Volume II.

- A system operating in the Compartmented or Multi-Level Security Modes should be using the information assurance level of effort addressed under the guidance in IA Publication 5239-13 Volume III.

- Systems that are identified as Mission Critical category I, II, or III should use the guidance provided in IA Publication 5239-13 Volume III.

Ultimately, the DAA and Certification Authority should decide on the best approach to define the level of risk in operating the system. IA Publication 5239-13 Volumes II and III are provided to aid in the implementation of the Certification and Accreditation process.

SECTION 5.0

REFERENCES

- NSTISSI 4009 - National Information Systems Security (INFOSEC) Glossary, January 1999
- NSTISSI No 4011 - National Training Standard for Information Systems Security (INFOSEC) Professionals
- NSTISSP Fact Sheet 11 – National Information Assurance Acquisition Policy, January 2000
- Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8519 “Department of Defense Global Information Grid Information Assurance, June 2000
- Department of Defense Information Technology Security Certification and Accreditation Process
- SECNAV 5239.3 – Department of the Navy Information Systems Security (INFOSEC) Program. (CH-1 dated 17 Jan 1997) and 14 July 95.
- OPNAVINST 5239.1B - Navy Information Assurance (IA) Program, 9 Nov 1999.
- DoN IA Publication 5239-01 - Introduction to Information Assurance (IA), May 2000.